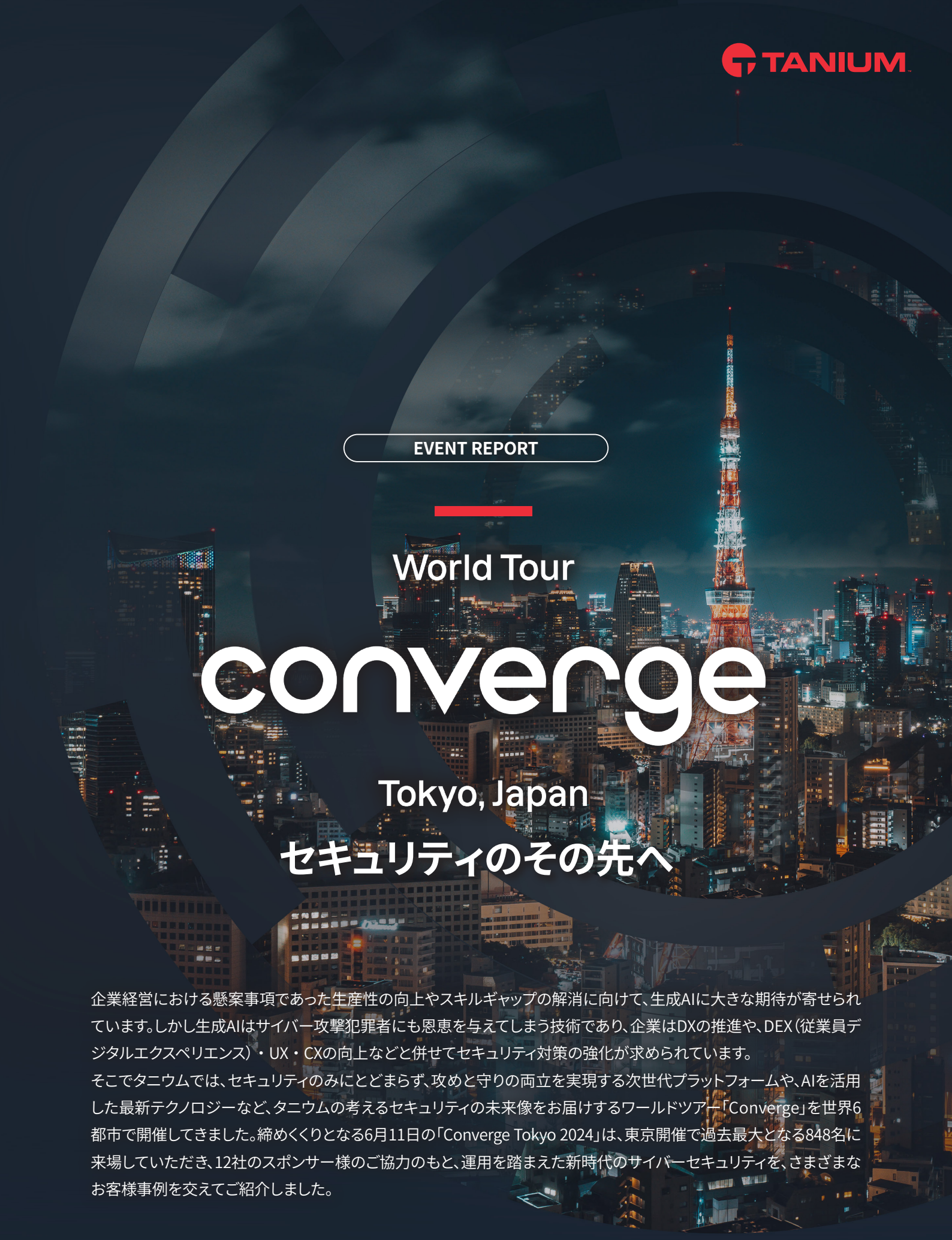


TANIUM

EVENT REPORT

World Tour converge

Tokyo, Japan

セキュリティのその先へ

企業経営における懸案事項であった生産性の向上やスキルギャップの解消に向けて、生成AIに大きな期待が寄せられています。しかし生成AIはサイバー攻撃犯罪者にも恩恵を与えてしまう技術であり、企業はDXの推進や、DEX（従業員デジタルエクスペリエンス）・UX・CXの向上などと併せてセキュリティ対策の強化が求められています。

そこでタニウムでは、セキュリティのみにとどまらず、攻めと守りの両立を実現する次世代プラットフォームや、AIを活用した最新テクノロジーなど、タニウムの考えるセキュリティの未来像をお届けするワールドツアー「Converge」を世界6都市で開催してきました。締めくくりとなる6月11日の「Converge Tokyo 2024」は、東京開催で過去最大となる848名に来場していただき、12社のスポンサー様のご協力のもと、運用を踏まえた新時代のサイバーセキュリティを、さまざまなお客様事例を交えてご紹介しました。

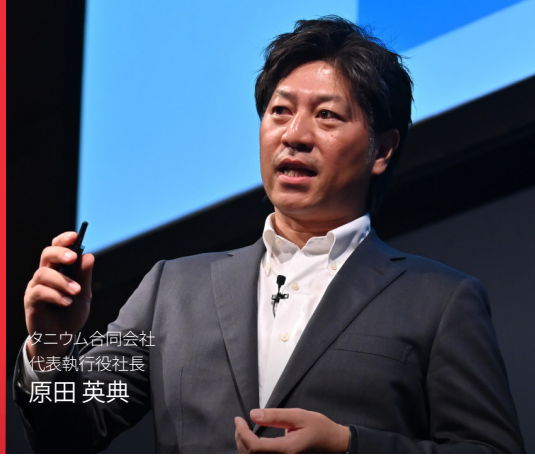
EVENT REPORT

World Tour

converge

Tokyo, Japan

セキュリティのその先へ



基調講演

多様化・巧妙化するサイバー攻撃を「自律型」で迎え撃つ Tanium XEMプラットフォームの価値

基調講演「高度化するサイバー脅威とデジタル変革をリードする新時代のサイバーセキュリティ」では、冒頭でタニウム代表執行役社長 原田英典が国内事業の近況を報告しました。2014年に事業を開始し、昨年の2023年に管理対象のエンドポイントが300万を超えて端末管理・セキュリティツールのクラウドソリューションにおいて国内シェア1位となったことや、IDCレポートに初登場し「Leader」に位置付けられたこと(*1)を伝えました。

続いて原田は「Convergeのコンセプトは一貫しています。それは、非常に多く誕生しているTaniumのユースケースを皆様に共有することです」とした上で、さっそくタニウムを幅広く活用するベネッセホールディングス様の事例を、壇上にお招きした同社専務執行役員 CDXO 橋本英知氏とともにご紹介しました。

同社はDXを進める中でグループ全体のエンタープライズアーキテクチャを再設計してきました。橋本氏は「クラウドやSaaSの活用で社外の皆様とのコラボレーションを進めなければなりません。また、リモートワークへの対応も必要です。攻めるためにも守りをしっかり固めることが重要です」と話した上で、脆弱性把握の強化のための全数端末可視化とサイバーハイジーンを実施していると説明します。その「守り」を下支えしているのがTaniumです。同社では生成AIの活用にいち早く取り組みはじめ、Microsoft Copilot Studioで社内業務の困りごとに対応するなど、業務の中でのさまざまな活用方法を創出しています。

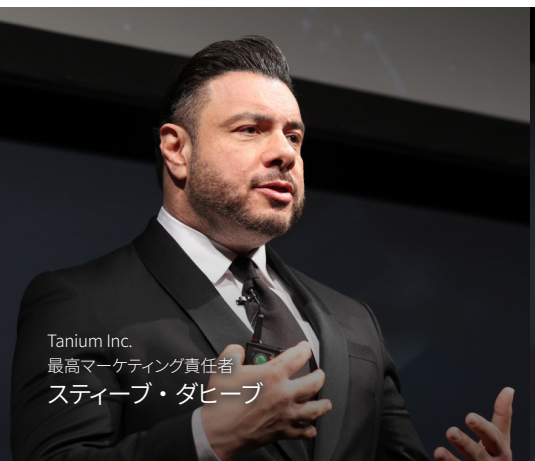
橋本氏は「AIのマルチモーダル化が進んで企業の優位性がなくなれば、データセットの整備や、顧客理解の上でどういう形でサービスの中に組み込んでいくのかが重要になってくると思いながら、さまざまなトライを進めている状況です」と語りました。

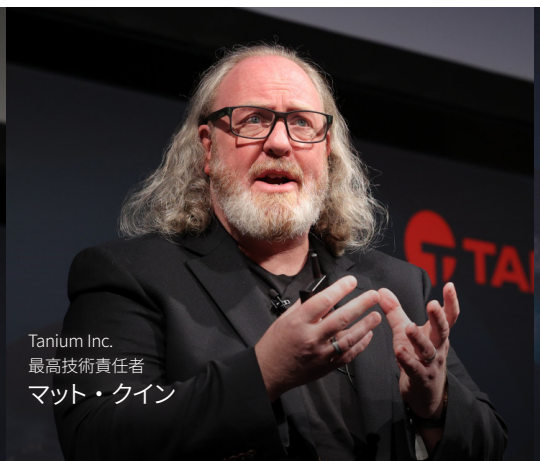
続いて壇上にはTanium Inc.最高経営責任者のダン・ストリートマンが上がり、「AIはより生産性を上げるだけではなく、同じアドバンテージを攻撃者に対しても提供します。私たちは防御に毎回成功する必要があります」と語り、Taniumはそれに対応するAI・自動化の基盤であることや、可視化、制御、そして是正の機能を単一のプラットフォームで提供している業界唯一の存在であることを強調しました。また、MicrosoftやServiceNowとのジョイントイノベーション推進、日本のパートナーエコシステム、お客様のストーリーについても説明しました。

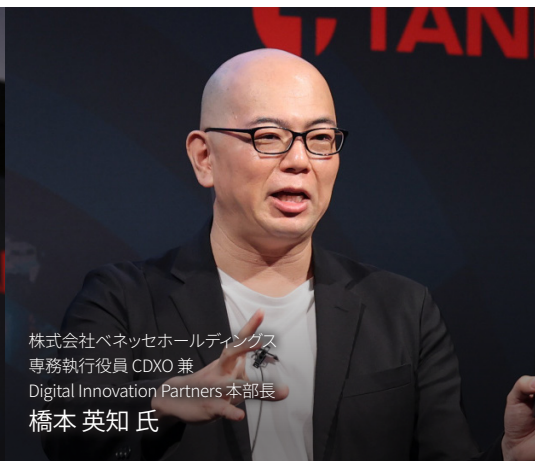
ストリートマンの次に登壇した最高マーケティング責任者のスティーブ・ダヒーブは、二刀流の剣術家・宮本武蔵が著した兵法書「五輪書」を紹介しながらTaniumの姿勢と共通点があることを語ります。その上でTaniumがIT運用とセキュリティ、可視化と対応、防御と攻撃の「二刀流」だと紹介しました。

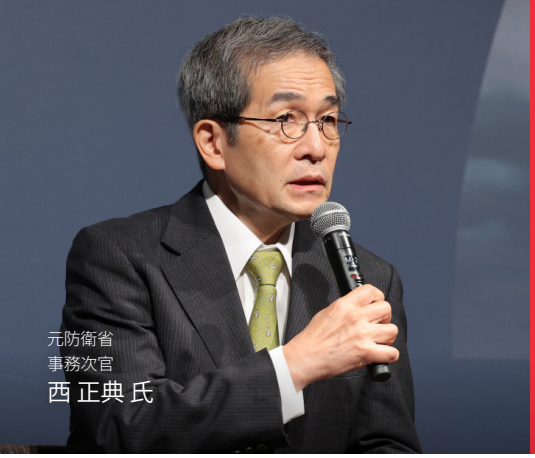
具体的なテクノロジーの紹介は最高技術責任者のマット・クインが引き受け、Tanium XEMが自律型エンドポイント管理であることなどを紹介し「自信を持って、適切なタイミングで適切なアクションを行えるようにすること、それが我々のゴールです」と述べました。

*1 Worldwide Client Endpoint Management Software for Windows Devices 2024 Vendor Assessment部門









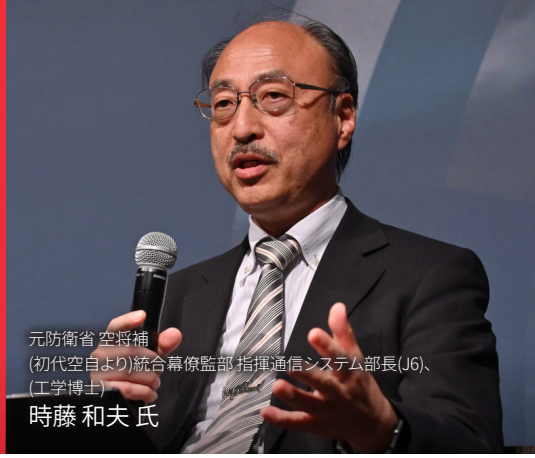
EVENT REPORT

World Tour

converge

Tokyo, Japan

セキュリティのその先へ



パネルディスカッション

経営の意志決定のもとサイバーハイジーンによるレジリエンス強化を

基調講演に続くパネルディスカッション「これからの日本に求められるセキュリティ対策とは？」では、まず、現状の安全保障上の脅威について認識を共有しました。

元防衛省空将補の時藤和夫氏は、「サイバー攻撃のインシデントが日常で報道されていると言われていますが、私は日本ではそのように感じません。海外の攻撃者グループによる活動が活発で脅威度は高いものの、あまり大きく議論されている印象がなく、認知度が低いように思います。その理由として、日本人の関心の低さ、インシデント情報を公開することへの恐れ、そして言語の壁があるのではないでしょうか。先ほどの基調講演では『スピード』や『変化』という言葉が何度も出てきましたが、それにどう対応するのかが問題です」と述べました。

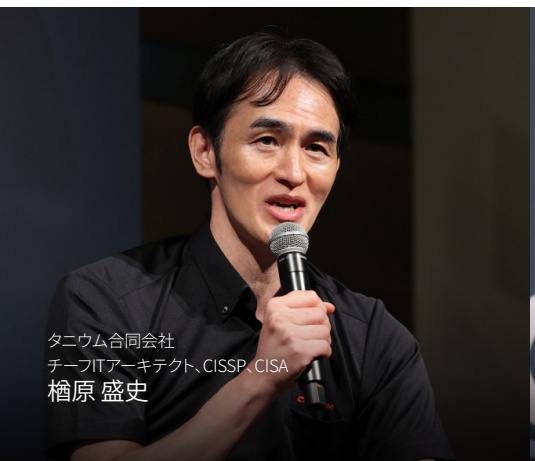
企業の脅威への備えについては、元防衛省事務次官の西正典氏が、一例として暗号通信の古い機械の中にはリスクが高いものが存在していることを指摘し、「欧米では一般の週刊誌でも暗号通信の古い機械による情報漏えいのニュースが取り上げられていましたが、日本のメディアでは報じられませんでした。リスクというものを軽く見てはいけません。リテラシーの問題として、足元をきちんと検証しましょう」と呼びかけました。

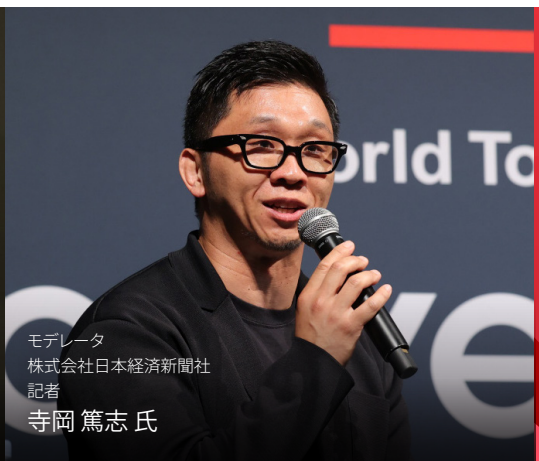
また、タニウムの楢原盛史はインフラが狙われる事例の増加に触れ、「最近多い事案は製造業のサーバーを狙ったものです。そして報道されているプライム上場企業の事故は97％がサプライチェーン経由であり、非常に大きな課題です」と分析します。

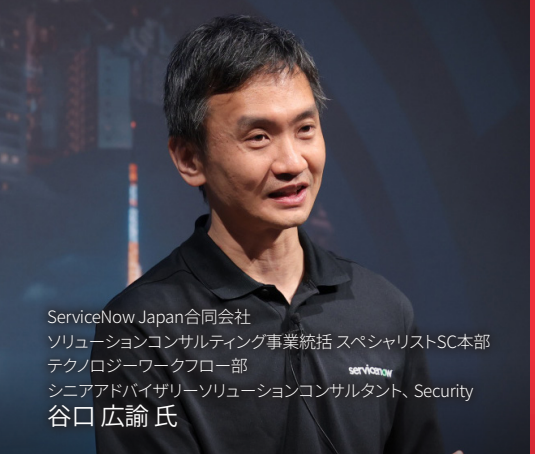
こうした状況に対して、どのような政策が取られているのでしょうか。西氏は「サイバーセキュリティが特殊なのは、国家主権による防御ができず、国も大企業も個人も無防備であることです。国や警察が守れない、いまだジャングルと同じだという認識を早く持つべきです」と説明します。

モデレータを務める日本経済新聞社の記者 寺岡篤志氏は、長年のセキュリティに関する取材経験でベストプラクティスを聞いたことがないものの、特にサプライチェーンセキュリティの自主的な活動では「資産管理が重要ではないか」と指摘します。これに対して楢原は「サイバーハイジーンでも資産管理、構成管理を徹底的に行うことが必要です。簡単ではありませんが、Taniumのリアルタイム性や自律性でカバーできます」と説明。また、最近のお客様は内部犯行の関心も高まっており、どのようにテクノロジーでカバーできるのかという議論も盛んであることに言及しました。

締めくくりとして西氏は「最後に運用している人間がリテラシーを高め、日常的に当たり前のことを当たり前に実現していけるかどうかで、かなりセキュリティは変わってくるでしょう」と語りました。時藤氏は「サイバーセキュリティに特効薬はなく、レジリエンスが重要です。意志決定する経営がしっかり入る必要があります」と強調し、それを受けて楢原は「ハイジーンなくしてレジリエンスはありません」と続けました。







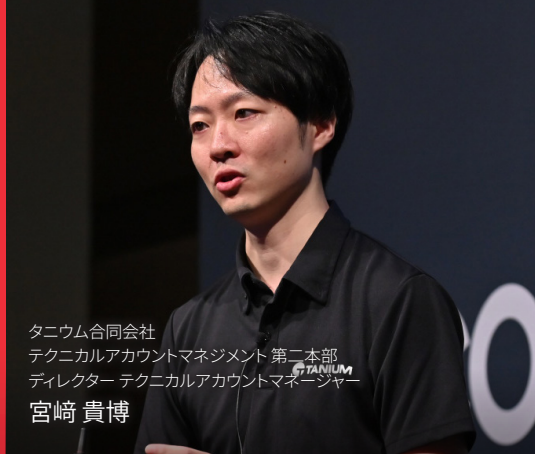
EVENT REPORT

World Tour

converge

Tokyo, Japan

セキュリティのその先へ



Tanium × ServiceNow

特別講演 Tanium＋ServiceNow

運用の自動化が セキュリティ対策の実効性を高める

特別講演「Tanium＋ServiceNowで実現する次世代自動化プラットフォーム」は、ServiceNow Japanとタニウムの2社で開催したセッションです。

はじめにServiceNow Japanの谷口氏は「1つひとつのソリューションで対応するのではなく、一気通貫で自動化することが必要だと常々考えています」と強調します。そしてServiceNowはITバリューチェーン全体をカバーする多彩な機能を持ちながらも、プラットフォーム上でデータを一元化できること、IT環境の可視化に欠かせない構成管理データベース（CMDB）を有することなどの特徴を紹介しました。

ServiceNowではTaniumのような脆弱性スキャナから取り込んだ情報をもとに、自動で優先度付け、修正タスク作成、担当への割当、リクエスト作成までを行います。また、パッチの自動対応やレポーティングも可能です。人間が対応を求められる場面は、例外リクエスト時などワークフローの一部のみとなり、対応工数や所要時間は大幅に短縮できます。

Taniumと連携するメリットについて谷口氏は、「大きく2つあります。Taniumはデータを取ってくるまでのレスポンスや確実性が優れており、CMDBを作るための主要なツールとなります。また、エンドポイントの脆弱性、リスク、コンプライアンスデータをまとめて運用することでセキュリティリスクを減らすのに重宝しています」と説明しました。

講演の後半では「ServiceNow谷口氏に聞く！Q&Aセッション」と題し、タニウムの宮﨑がお客様と接する中でくみ取った「Tanium＋ServiceNowで気になること」を挙げ、谷口氏とともに答えました。

――Taniumとの連携でServiceNowの追加ライセンスは必要？

「基本ライセンスは必要ですが、ServiceNow Storeで提供される9個の機能（Connector）はTanium Security Operationsに含まれています。（一部例外はあります）」（宮﨑）

――Taniumの情報収集とServiceNowの情報収集はどのように違う？

「機能が被っているけれど競合ではありません。ServiceNowは中間サーバーからスキャンして1カ所に収集する仕組みで、エージェントも提供していますが入れることにこだわっていません。Taniumはエージェントで効率的に収集でき、歓迎すべきパートナーです」（谷口氏）

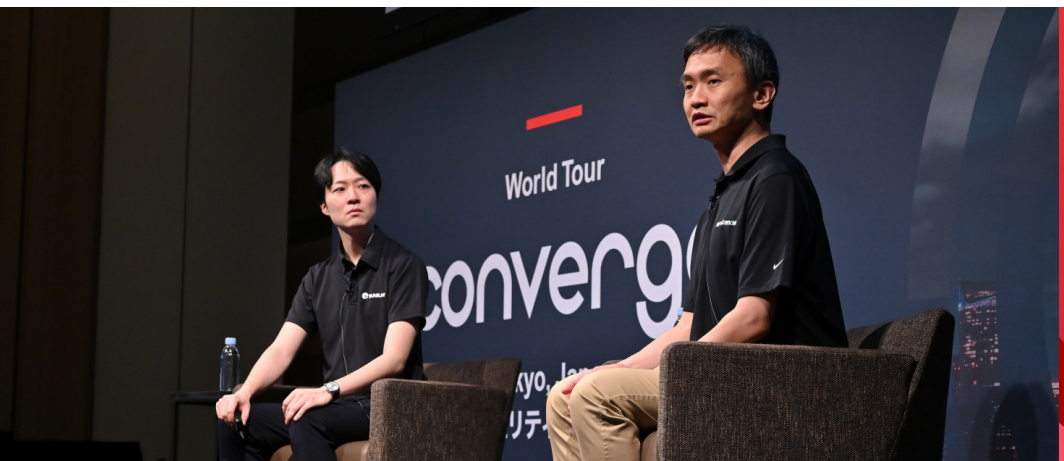
――脆弱性管理はTaniumとServiceNowの連携でどのように良くなる？

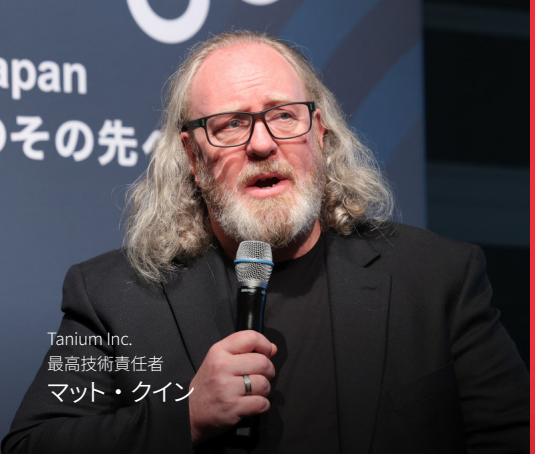
「脆弱性を見つけると、他のスコアや資産情報も交えて評価しやすくなります。また、即座に担当者をアサインして対応するなど“セキュリティのその先”を見据えた運用が可能になります」（宮﨑）

――ズバリ！ServiceNowから見てTaniumのすごいところは？

「『面』で対応するので、感染の拡大によって脆弱性が横展開するのを防ぐことができます。またリアルタイム性もあるため、今すぐ取りかかるべき問題にも対応できます」（宮﨑）

「クライアント管理のデファクトだと思っています」（谷口氏）





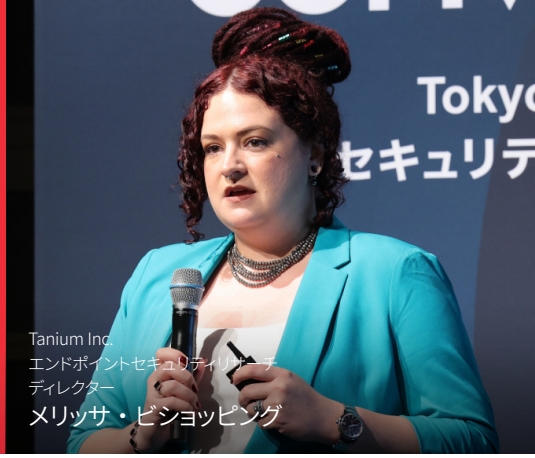
EVENT REPORT

World Tour

converge

Tokyo, Japan

セキュリティのその先へ



ロードマップセッション N-1

現行モジュールの意欲的な投資を続けながらプラットフォームの将来像を描く

基調講演で触れたTanium XEMの方向性をより詳細に説明する「Taniumで実現するAI時代のIT・セキュリティ運用の両立」と題したこのセッションでは、まず直近の機能強化についての情報を共有しました。「特にこの3つを強調したい」とTanium Inc. 最高技術責任者のマット・クインが挙げたのは、Enforce（ゼロトラスト用のEntra ID連携）、SBOM for Comply（ソフトウェア サプライチェーンリスクの可視化）、Endpoint Reactions（発見されたエンドポイント脅威への対応自動化）です。

続いて製品およびモジュールレベルでの製品ロードマップを4つ紹介しました。

①エンドポイント管理では、「Patch」でのパッチ配信時の帯域幅の最適化、「Deploy」でのソフトウェアカタログの最適化とデプロイメントの自動化、「Enforce」でのBitlocker & Filevaultの設定による暗号化管理の強化を予定しています。

②従業員デジタルエクスペリエンスについてクインは、「パフォーマンスメトリックをより大きなものにしていきたいと考えています」と語りました。「Performance」では即時解決のためのプロアクティブなアラート機能、パフォーマンスに関する問題のストリームサポートを実装予定です。また、「Engage」では多言語対応、macOSでのユーザのセルフヘルプをサポートする計画となっています。

③リスク&コンプライアンスに関しては、「引き続き多くの投資を行っております」とした上で、「Comply」のコンテナイメージの脆弱性スキャンに説明しました。

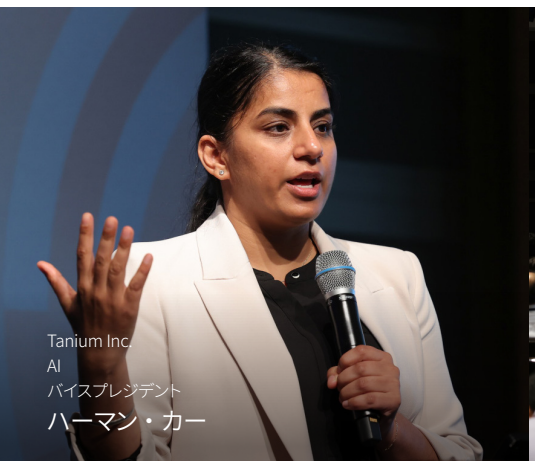
④インシデントレスポンスでは、お客様からの要望が多かった「Threat Response」のオンデマンドの脅威ハンティングなどが可能になります。

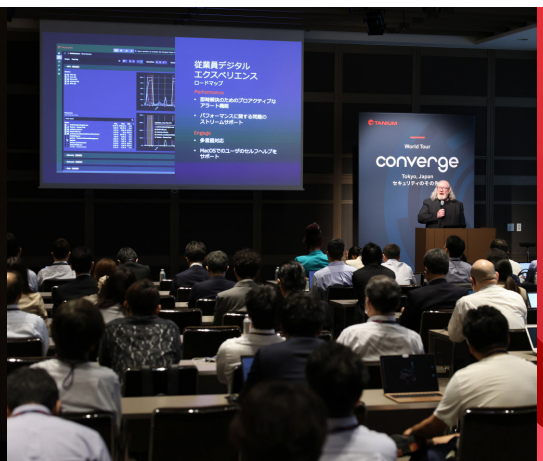
ここでクインは「皆様がいま使っているモジュールであっても投資を続けていき、皆様の声に耳を傾けてプラットフォームを前進させていきます」と強調しました。

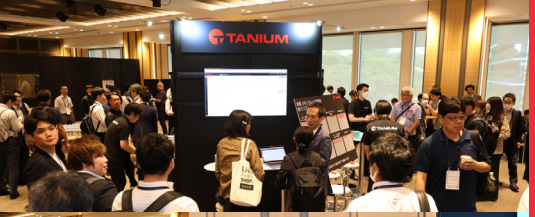
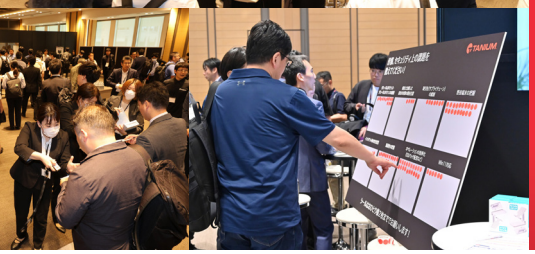
紹介するロードマップの対象はCore Platformへと進み、エンドポイントの多様化、エコシステムの統合、そして自律型エンドポイント管理の3つの要素について多くの投資を行うことを表明しました。

その中でリアルタイムデータを人間の知性でいかに強化して実用的なインサイトを提供するのかというテーマでは、同社エンドポイントセキュリティリサーチ ディレクターのメリッサ・ビショッピングが、ビジネス側のニーズも視野に入れた適応性と、実践的なセキュリティ対策とするための汎用性について詳しく語りました。

また、自律型エンドポイント管理については、同社AIのバイスプレジデントを務めるハーマン・カーがその必要性を可視化、制御、是正の3点で説明した上で深掘りしました。





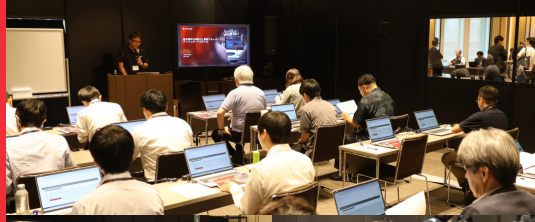
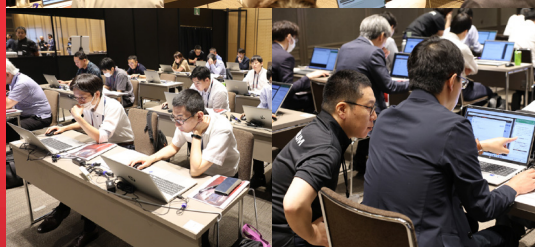
EVENT REPORT

World Tour

converge

Tokyo, Japan

セキュリティのその先へ

セキュリティ課題の関心から
来場者が絶えなかった展示やデモのコーナー

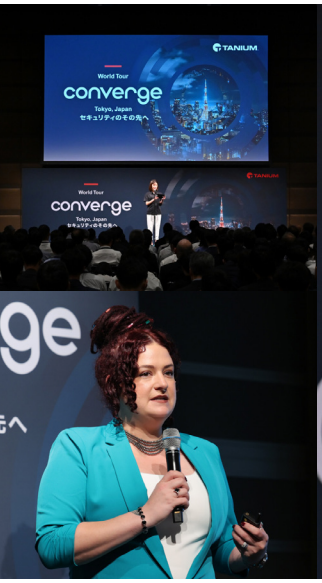
タニウムの展示コーナーには、多くのお客様にお立ち寄りいただきました。タニウム初となる書籍『Taniumで始めるサイバーセキュリティ ～ サイバーハイジーン徹底解説』を配布したところ、配布開始から2時間あまりで500冊以上を手に取っていただきました。

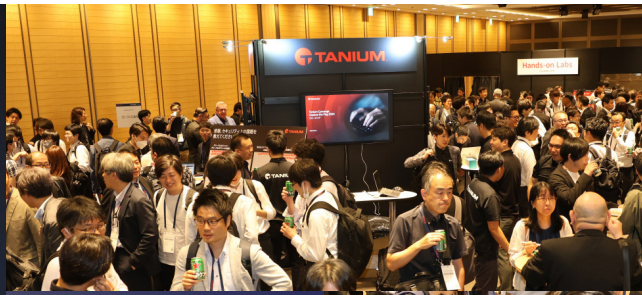
Tanium製品ご紹介＆デモコーナーでは、いま直面している課題をTaniumで解決できるのか？具体的にTaniumでどこまでできるのか？など、Taniumの導入や活用に関する疑問に、タニウムのエキスパートがデモなどを交えてお答えしました。

デモコーナーの一角では、セキュリティ上の課題を尋ねるボードを設置し、8つの代表的な課題のうち当てはまるものにシールを貼っていただいたところ、「脆弱性の把握」、OSパッチ配信など「オペレーションの効率化」、「野良端末の把握」に多くのシールが集まりました。シールはお一人様2枚までとさせていただいたため、該当する課題が多すぎて悩む様子も見られました。

今回のConverge Tokyoでは、日本で初めてオンサイトでの「ハンズオンラボ」も開催しました。初めてTaniumに触る方でも参加可能な「端末運用の高度化に貢献するレポートやダッシュボードの作り方」や、Taniumの基本操作習得者が対象の「新機能Tanium Automateを使ったワークフローの設定」、中級者向けの「Tanium ComplyとSBOMを使い、組織に内在する脆弱性（ComplyとSBOMを利用）を見つけ出す方法」の3種類を用意し、各回20席の参加チケットを基調講演終了後に配布したところ、5分後には配布終了となってしまう盛況ぶりでした。

また、サイバーセキュリティの技術を競うイベントの「CTF（Capture The Flag）チャンピオンシップ大会」が同時開催され、過去国内で開催されたCTF大会の成績上位5チームがTaniumを使って競いました。





お問い合わせ

TANIUM

タニウム合同会社
〒100-0004　東京都千代田区大手町2丁目6－4 常盤橋タワー25 階

https://www.tanium.jp
jpmarketing@tanium.com